CYBER SECURITY

IN 2021

JAKE ADSHEAD

CYBER SECURITY CONSULTANT

jake.adshead@maxwellbond.co.uk

maxwellbond

maxwellbond

Introduction

Exploring SIEMS, Teams, and Managed SOCs

After a challenging year in 2020, businesses are now busy preparing for whatever 2021 might bring. Cyber Security is no exception. In 2020, cyber threats increased and became more malicious and sophisticated than ever before, taking advantage of the vulnerabilities linked to remote and home working.

I sat down with Cyber leaders to discuss some of the challenges and topics they think have become fundamental to their business' information and cyber security as we wade through 2021. Get in touch for more information on future roundtables or advice and guidance on building or maturing your cyber security function.

Contents

maxwellbond

SIEM Systems

A SIEM system uses machine-generated data to get operational insights into threats, vulnerabilities, security technologies, and to identity information. SEIM platforms, such as Splunk, used to be something everyone was eager to invest in, but is this still the case, or are leaders looking more down UVA and network layering?

From the discussion it became clear that most businesses seemed to still rely on some form of SIEM platform, and the real difference came with business requirement and preference. The platforms that came up most frequently were Splunk, Darktrace, and Rapid7's InsightIDR tools, which all vary in their levels of cost, automation, and training requirements.

The immediate point raised was the expense in both time and cost for a platform like Splunk, which is not only extremely expensive (one of the most expensive), and also time consuming to use, but it's also very hard to recruit for, which means you spend even more in recruitment and training. It can take a significant amount of time to learn how to effectively set up your own correlations, searches, and reports on Splunk, as all of this has to be done manually. It can be an extremely steep learning curve and is therefore not suitable as an out of the box solution.

Darktrace is another popular choice for businesses, although its biggest critique is that whilst it looks "flashy", but it doesn't quite go deep enough on deep packet inspections and other important practices.

Whilst SIEMs can definitely add value in terms of enabling instant response to threats and attacks, it's worth considering the architectural complexity of your network, your requirements, topologies and available resources before deciding on a tool. For example, one more affordable "out of the box" solution is Rapid7's InsightIDR, which does most of the tuning and the heavy lifting, including automatically completing configurations and cross log searches and anomaly detection. This means there is less of a pressure on business resources and time and it's a great option for businesses who invest in junior cyber talent.

Managed SOCs

Managed SOC, also known as SOC as a Service, is a subscription-based offering whereby organizations outsource threat detection and incident response. It can sometimes be seen as a good option for those without an in-house security team.

Using a managed SOC has benefits around time, resources and cost, which is important for smaller cyber teams or during times, such as COVID, when cyber teams might be experiencing redundancy and cutbacks. If you choose a good provider, you are effectively extending your team and passing some of the workload over to external experts who can closely monitor threats, send alerts to enable rapid incident response and event investigation, and just decreases pressure on cyber teams who might already be under stress.

However, a Managed Security Solution (or SOC) can be detrimental in a number of ways to businesses, namely that they often lack a complete understanding of your environments because they are so separate and distant from your business. Because they manage multiple SOC's for different businesses, you won't necessarily always be priority. Additionally, if you opt for a Managed SOC from a different country, there may also be language and cultural barriers that make effective communication much more difficult.

Automating as much as possible is often preferable to using managed SOC's, as it allows you to maintain full control and visibility, whilst most of the work is done with minimal manual input. There is, however, cost and training implications here too.

COVID-19 & Teams

COVID-19 has affected businesses in different ways, so it's no surprise that each cyber security function will have been impacted differently, depending on the business and sector in which they sit. Some businesses will have been lucky enough to continue with a "business as usual" mindset, whilst others will have faced mass redundancy or furlough.

For those who have lost team members, permanently or temporarily, smaller teams often find themselves working overtime and managing a high workload between a few members of staff. For some this has meant they have had no option but to outsource some of their security workload in order to keep up with testing, analysing and responding to any threats, whilst also keeping up with the operational side of security.

As I mentioned previously, automating as many processes as possible is preferable to outsourcing in many scenarios, however, time and costs may be a barrier to this.

maxwellbond

Embedding Testing into the Development Lifecycle

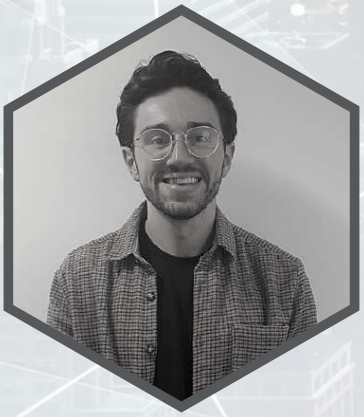
Embedding security testing into agile software development, means that quality isn't just tested afterwards, it is built in and tested constantly throughout the full development lifecycle. With the right practices and the right set of tools, you can make sure that you build secure apps in a frictionless way and eliminate unpleasant and expensive security surprises that may affect your applications usability, security, and reputation after the release.

The maturity of a development lifecycle will depend on the type of business that it sits within. More mature lifecycles will introduce more cyber security testing at a granular level, whilst less mature functions will not. Having a Quality Assurance Document will help businesses understand what they should be doing (e.g., in terms of penetration testing, code reviews, and cyber training) even if they are not at a stage of actually implementing it yet.

Whilst embedded security testing can help prevent security issues with the live application, it does pose a number of challenges around hardware dependency, defected ratio, unreproducible defects, and software updates. There are also the common challenges faced when implementing any new processes, and it can take a while for teams to get up to date with what their roles are in a new environment.

Contact Us

Build high performing teams through exceptional contract and perm staffing solutions and business advice with Maxwell Bond, the recruitment partner of choice across the UK and Germany.



Jake Adshead
Senior Cyber Security Consultant
jake.adshead@maxwellbond.co.uk
0161 359 3280

Find out more at www.maxwellbond.co.uk